(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/000397 A1

(51) International Patent Classification[7]: A61N 1/372, 1/08, A61B 5/00, G06F 19/00, H04L 9/30, 9/32, 9/08

(21) International Application Number: PCT/US2004/019902

(22) International Filing Date: 22 June 2004 (22.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/601,763 23 June 2003 (23.06.2003) US

(71) Applicant (*for all designated States except US*): CARDIAC PACEMAKERS, INC. [US/US]; 4100 Hamline Avenue North, St. Paul, MN 55112 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): VON ARX, Jeffrey, A. [US/US]; 2115 Emerson Avenue South, Minneapolis, MN 55405 (US). KOSHIOL, Allan, T. [US/US]; 6630 Ruffed Grouse Road, Lino Lakes, MN 55014 (US). BANGE, Joseph, E. [US/US]; 832 Overlook Place, Eagan, MN 55123 (US).

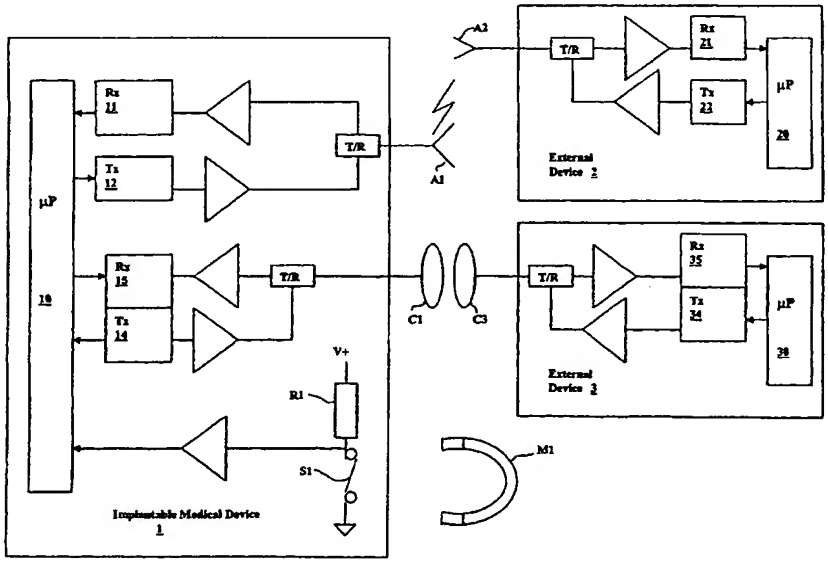
(74) Agents: STEFFEY, Charles, E. et al.; Schwegman, Lundberg, Woessner & Kluth, P.O. Box 2938, Minneapolis, MN 55402 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE TELEMETRY FOR IMPLANTABLE MEDICAL DEVICE



(57) Abstract: A method and system for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel. A telemetry interlock may be implemented which limits any communications between the ED and the IMD over the telemetry channel, where the telemetry interlock is released when the ED transmits an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD. As either an alternative or addition to the telemetry interlock, a data communications session between the IMD and ED over the telemetry channel may be allowed to occur only after the IMD and ED have been cryptographically authenticated to one other.

WO 2005/000397 A1

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SECURE TELEMETRY FOR IMPLANTABLE MEDICAL DEVICE

Field of the Invention

This invention pertains to implantable medical devices such as cardiac pacemakers and implantable cardioverter/defibrillators. In particular, the invention relates to a system and method for transmitting telemetry data from such devices.

Background

Implantable medical devices (IMDs), including cardiac rhythm management devices such as pacemakers and implantable cardioverter/defibrillators, typically have the capability to communicate data with an external device called an external programmer via a radio-frequency telemetry link. One use of such an external programmer is to program the operating parameters of an implanted medical device. For example, the pacing mode and other operating characteristics of a pacemaker are typically modified after implantation in this manner. Modern implantable devices also include the capability for bidirectional communication so that information can be transmitted to the programmer from the implanted device. Among the data that may typically be telemetered from an implantable device are various operating parameters and physiological data, the latter either collected in real-time or stored from previous monitoring operations.

External programmers are commonly configured to communicate with an IMD over an inductive link. Coil antennas in the external programmer and the IMD are inductively coupled so that data can be transmitted by modulating a radio-frequency carrier waveform which corresponds to the resonant frequency of the two coupled coils. An inductive link is a short-range communications channel requiring that the coil antenna of the external device be in close proximity to the IMD, typically within a few inches. Other types of telemetry systems may utilize far-field electromagnetic radiation or other types of data links such as telephone lines or networks (including the internet) to enable communications over greater distances. Such long-range telemetry

allows the implantable device to transmit data to a remote monitoring unit or be programmed from a remote location. Long-range telemetry thus allows physicians to monitor patients and to conduct patient follow-ups from across the room or even across the world.

Long-term telemetry for implantable medical devices, however, causes some special concerns which are not present with short-range telemetry. Communication with an implantable device over a short-range communications channel such as an inductive link requires that the external device be near the patient, so that the clinician knows whose implantable device is being programmed and the patient knows who is programming and receiving data from the implantable device. Long-range telemetry, on the other hand, does not require such physical proximity and allows the possibility of a physician inadvertently programming the wrong device. Communications with far-field electromagnetic radiation or over some kind of network also allows the communications to be intercepted by an unintended user, raising privacy concerns for the patient. A malicious user might even try to use the long-range telemetry system to re-program an implanted device. The present invention is a system and method for providing long-range telemetry which addresses these concerns.

Summary

The present invention relates to a method and system for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel. In one embodiment, a telemetry interlock is implemented which limits any communications between the ED and the IMD over the telemetry channel. The telemetry interlock is released when the ED transmits an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD. In another embodiment, a data communications session between the IMD and ED over the telemetry channel is allowed to occur only after the IMD and ED have been authenticated to one other. The IMD is authenticated to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD, and the ED is authenticated to

the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED.

Brief Description of the Drawings

Fig. 1 is a block diagram of an exemplary telemetry system for an implantable medical device.

Fig. 2 illustrates a secret key authentication protocol.

Fig. 3 illustrates a public key authentication protocol.

Fig. 4 illustrates a particular public key authentication protocol.

Detailed Description

The present invention relates to a long-range telemetry system for implantable medical devices which guards against the possibility of malicious or inadvertent re-programming of an implanted device. In another aspect, the system may also provide for maintaining the confidentiality of data transmissions. Ensuring such patient safety and confidentiality may be accomplished using three separate techniques: encryption of data, authentication of the participants in a telemetry session, and telemetry interlock.

1. Encryption/Decryption

Encryption refers to cryptographic algorithms which are used to encode messages in such a way that they cannot be read without possession of a special key that decrypts the message. Encryption of a message is performed by applying an encryption function to the message, where the encryption function is defined by a cryptographic algorithm and an encryption key. In the following descriptions and referenced drawings, such an encrypted message will be designated as E(m,k), where E is the encryption function, m is an unencrypted message, and k is the key used to encrypt the message. Decryption of a message involves the application of a reverse function D to an encrypted message m using a decryption key k, designated as D(m,k).

The encryption and decryption keys may be the same or different depending upon the type of cryptographic algorithm which is used. In secret key cryptography, both participants in a communication share a single secret key which is used for both encryption and decryption of a message. Thus a message m encrypted by a secret key encryption function E with a key k is recovered by applying the decryption function D with same key k:

$$m = D(E(m,k),k)$$

Well-known examples of secret key cryptographic algorithms are DES (Data Encryption Standard), AES (American Encryption Standard), triple-DES, and Blowfish.

In public key cryptography, on the other hand, the encryption and decryption keys are different. In order to send a secure message using public key cryptography, the sender encrypts the message with the recipient's public key which is known to all authorized senders and may be widely-known to allow anyone to send a message. The message can then only be decrypted by the private key which corresponds to the public key used to encrypt the message, the private key being held by the message recipient and shared with no one else. Thus, a message encrypted with a public key encryption function E with a public key k1 is recovered by applying the decryption function D with the corresponding private key k2:

$$m = D(E(m,k1),k2)$$

Each participant in a secure two-way communications session must therefore possess its own private key and know the other's public key. A well-known example of a public key cryptographic algorithm is RSA.

Although either public key or secret key cryptography may be used to securely transmit data, public key cryptographic algorithms are much more computationally intensive. For this reason, it would usually be preferable to use secret key cryptography for the actual data communications between an implantable device and an external device. As explained below, however, public key cryptography may be advantageously used for authentication and to transmit the secret keys used for the data communications.

2. Authentication

Authentication refers to the mechanisms or protocols by which the participants in a communications session may reliably identify one another. An authentication protocol may be implemented using either secret key or public key cryptography to allow an implantable medical device (IMD) and an external device (ED) to authenticate one another. A data communications session between the IMD and ED over the telemetry channel is allowed to occur only after the IMD and ED have been authenticated to one other. With authentication by either public key or secret key cryptography, the IMD is authenticated to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD, and the ED is authenticated to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED.

In authentication by secret key cryptography, the IMD is authenticated to the ED when the ED transmits a first message to the IMD over the telemetry channel and receives in response a message derived from the first message which is encrypted by a secret key expected to be possessed by the IMD. The ED is then authenticated to the IMD when the IMD transmits a second message to the ED over the telemetry channel and receives in response a message derived from the second message which is encrypted by a secret key expected to be possessed by the ED.

An authentication protocol employing public key cryptography would work as follows. The IMD is authenticated to the ED when the ED encrypts a first message with a public key having a corresponding private key expected to be possessed by the IMD, transmits the encrypted first message over the telemetry channel to the IMD, and receives in response a message from the IMD derived from the first message which evidences possession of the corresponding private key by the IMD. The ED is authenticated to the IMD when the IMD encrypts a second message with a public key having a corresponding private key expected to be possessed by the ED, transmits the encrypted second message over the telemetry channel to the ED, and receives in response a message from the ED derived from the second message which evidences

possession of the corresponding private key by the ED. The messages derived from the first and second messages may include the first and second messages, respectively, along with identifying data such as identity codes for the ED and IMD. Rather than having separate transmissions for each, the IMD may transmit the message derived from the first message and the second message as a combined message (i.e., the message derived from the first message which is transmitted by the IMD would then include the second message). In one embodiment, the first and second messages include random numbers generated by the ED and IMD, respectively. The messages derived from the first and second messages would then either include the respective random number itself or a number derived therefrom (e.g., the random number incremented by one). In order to maintain confidentiality of the responses which authenticate one participant to the other, the messages derived from the first and second messages and which are transmitted by the IMD and ED, respectively, may be encrypted using the public keys of the ED and IMD, respectively.

3. Telemetry interlock

As explained above, cryptographic techniques may be used both to authenticate the IMD and ED to one another and to securely transmit data. All cryptographic techniques, however, depend upon either the secret key or private key being kept secret. In order to give the patient added security with respect to long-range telemetry, a technique referred to herein as a telemetry interlock is employed. A telemetry interlock is a technique which limits any communications between the ED and the IMD over the long-range telemetry link until the interlock is released. The telemetry interlock is released by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD. . In one embodiment, no information at all is allowed to be transmitted until the interlock is released. This is the more secure embodiment. In a second embodiment limited information is allowed, but programming of the device is not. This embodiment supports remote patient monitoring without the patient having to release the interlock.

One way of implementing the telemetry interlock is to use an inductive link as the short-range communications channel. As noted above, traditional implantable medical devices have an inductive telemetry link that is very short range (just a few inches). In this implementation of a telemetry interlock, the IMD hardware will require that an inductive link be established with keys exchanged inductively to release the long-range telemetry interlock. In one embodiment the release of the telemetry interlock would time out after a few tens of minutes, and again a wave of the inductive wand over the device would be needed to continue the session. In another embodiment the telemetry interlock would not expire until the end of the current telemetry session.

Another way of implementing the telemetry interlock is to use the static magnetic field of a magnet as a short-range communications channel so that the telemetry interlock is released when a magnet is held near the IMD. This embodiment may be needed in cases where the IMD is not equipped with an inductive telemetry system. The doctor or other person trusted by the patient would then be required to wave a magnet over the implantable medical device to enable programming. Again the release of the interlock would expire after either some short duration of time or at the end of the present telemetry session.

Both of these interlock techniques will stop malicious programming from a remote hacker because the interlock can only be released by someone physically very close to the patient. These interlock techniques will also stop unintentional programming by a valid user. Because a doctor or other authorized user may accidentally establish a telemetry session with the wrong device (long range telemetry will allow multiple patients to be in range of a doctor's programmer), having to wave an inductive wand or magnet over the device to enable programming would prevent the doctor from accidentally programming the wrong device.

4. Secure data communications session

Once authentication and release of the telemetry interlock have occurred, the IMD and the ED can proceed to communicate data over the long-range telemetry link

with each device knowing that the other is not an impostor. If the data is sent in the clear during the data communications session, however, an eavesdropper could intercept the data and compromise the patient's privacy. It may therefore be desirable to encrypt some or all communications between the ED and the IMD during the data communications session. As stated earlier, secret key encryption is much less computationally intensive than public key encryption and is preferred for transmitting relatively large amounts of data. If secret key cryptography is used for authentication, the ED and IMD can use the same secret key for data transmission. If public key cryptography is used for authentication, secret key cryptography can be used for data communications, where one of either the ED or the IMD transmits to the other of either the ED or the IMD a secret session key encrypted by the latter's public key. That secret session key can then be used by both participants to encrypt data.

4. Exemplary hardware description

Fig. 1 is a block diagram of the telemetry components of an implantable medical device 1 and two representative external devices 2 and 3. Each of the devices has a microprocessor or other type of controller designated 10, 20, or 30 for processing the digital data. Software or firmware executed by the controller in each device may implement various communications algorithms and protocols when transmitting or receiving messages, including the encryption, authentication, and telemetry interlock schemes described above. A data receiver and a data transmitter are interfaced to the controller in each of the devices for receiving and transmitting either a modulated carrier signal or a baseband signal. A demodulator or decoder for extracting digital data from the carrier signal or baseband signal is incorporated into each receiver. A modulator or encoder is incorporated into each transmitter for modulating the carrier signal with digital data or encoding the baseband signal. The data transmitted by each of the devices is digital data that can be transmitted directly as baseband data in certain types of data links or as a modulated carrier signal. In either case, the data is transmitted in the form of symbols representing one or more bits of information. For example, in on-off amplitude shift keying, each pulse represents either a one or a zero.

Other modulation methods (e.g., M-ary modulation techniques) utilize symbols representing a greater number of bits.

Each of the external devices 2 and 3 would typically be an external programmer which can both re-program and download data from the implantable device 1. The external device 3 is intended to represent a device designed for short-range telemetry via an inductive link where a coil C3 is interfaced to the receiver 35 and transmitter 34 for inductively linking with a corresponding coil C1 interfaced to the receiver 15 and transmitter 14 of the implantable device. The coil C3 would typically be incorporated into a wand for positioning close to the implantable device, while the coil C1 is typically wrapped around the periphery of the inside of the implantable device casing. An example of an inductive link telemetry system for an external programmer and a cardiac pacemaker is described in U.S. Patent No. 4,562,841, issued to Brockway et al. and assigned to Cardiac Pacemakers, Inc., the disclosure of which is hereby incorporated by reference. The external device 2 is intended to depict a device which communicates with the implantable device 1 over a long-range telemetry link, implemented with either far-field radio transmissions or over a network. For transmitting and receiving data between the devices over the long-range telemetry link, a data receiver 11 and a data transmitter 12 are interfaced to the controller in the implantable device 1, and a data receiver 21 and a data transmitter 22 are interfaced to the controller in the external device 2. In the case of a far-field radio link, the receiver/transmitter pair of the implantable device 1 and external device 2 are interfaced to antennas A1 and A2, respectively. In the case where long-range telemetry is implemented over a network, the receiver/transmitter pair of external device 2 would be interfaced to a network connection, while the implantable device would 1 would be wirelessly interfaced to a repeater unit with a network connection.

The implantable device 1 is also equipped with a magnetically actuated switch S1 and associated pull-up resistor R1 which is interfaced to the controller 10. In this embodiment, the telemetry interlock may be released by either a command transmitted from the external device 3 over the inductive link formed by the coils C1 and C3 or by actuation of the switch S1 by proximity of an external magnet M1 may be used to

release the telemetry interlock. In other embodiments, the implantable device would perhaps only have one type of short-range communications channel for releasing the telemetry interlock, either a magnetically actuated switch or an inductive link telemetry system. Other types of short-range communications channels for releasing the telemetry interlock are also possible, including short-range telemetry systems implemented with a capacitive link or a physically actuated switch.

5. Exemplary specific embodiments

As described above, a system in accordance with the invention for providing secure long-range telemetry for an implantable medical device may include any one or all of the following: 1) a telemetry interlock released via a short-range communications channel, 2) an authentication protocol by which an external device and the implantable device can identify one other, and 3) encryption of the long-range telemetry communications to ensure patient privacy. The following are descriptions of exemplary schemes which incorporate those features.

In one particular embodiment, the telemetry interlock technique described above is used as the sole means for providing security before the initiation of a long-range telemetry session, with no cryptographic authentication protocols being employed and the data sent in the clear. In another embodiment, only cryptographic authentication is used to provide security for initiating a long-range telemetry session, with no use of a telemetry interlock. In either of these embodiments, a long-range telemetry session can either be prevented entirely or limited to particular types of data transfers if no release of the telemetry interlock or cryptographic authentication occurs. For example, while it would probably not be desirable to allow an external device to program an implantable device via long-range telemetry without either release of a telemetry interlock or cryptographic authentication, certain types of data could still be allowed to be transferred from the implantable device, either with or without encryption. In another embodiment, neither cryptographic authentication nor a telemetry interlock is employed, but the implantable device uses either public key or

secret key encryption to send certain types of data to an external device over a long-range telemetry link.

One example embodiment of a method or system for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel includes a telemetry interlock which limits any communications between the ED and the IMD over the telemetry channel, where the telemetry interlock is released by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD. The IMD is authenticated to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD, and the ED is authenticated to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED. A data communications session between the IMD and ED over the telemetry channel is then allowed to occur only after the IMD and ED have been authenticated to one other. Either public key or secret key cryptography can be used for the authentication. In another example embodiment, secure communications between IMD and an ED over a telemetry channel is provided solely by a telemetry interlock which is released by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD, where data communications between the IMD and ED over the telemetry channel is limited until the telemetry interlock has been released.

In another example embodiment, secure communications between an IMD and an ED over a telemetry channel is provided by authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD, authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED, and allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD has been authenticated to the ED. In another embodiment, unilateral authentication is employed so that only one of either the IMD or the ED needs to be authenticated to the other before a data communications session is allowed to occur. For example, when an ED communicates

with an IMD, it may authenticate the IMD so that the ED knows that it is gathering data from the correct device. However, the IMD may not need to authenticate the ED unless the ED tries to alter its state (re-program it). As long as the ED is only reading data, there is no safety concern (although there may be a privacy concern).

Fig. 2 depicts a communications session between the external device 2 and the implantable device 1 over a long-range telemetry channel in an embodiment using a telemetry interlock and where authentication is performed with secret key cryptography. After the telemetry lock is released by an ENABLE command from the external device 3, the external device 2 transmits a message M1 encrypted by a secret key encryption algorithm using a key K1. The implantable device 1 responds by decrypting the message to obtain M1, modifying M1 in an agreed upon manner (e.g., incrementing the number M1 by one) to obtain M1*, transmitting M1* back to the implantable device encrypted by the key K1. After decrypting the message to obtain M1*, the external device 2 has authenticated the implantable device 1, as the latter has evidenced possession of the secret key K1. The implantable device 1 at the same time sends a message M2 encrypted by secret key K1. The external device 2 responds by decrypting the message to obtain M2, modifying M2 to obtain M2*, and transmitting M2* encrypted with key K1 back to the implantable device 1, thus authenticating the external device 2. The implantable device 1 then transmits a secret session key SK encrypted by key K1. A data communications session may then ensue in which DATA is transmitted by either of the devices encrypted with the secret session key SK. In another embodiment, data is exchanged between the devices during the data communications session using the same secret key K1 as used for authentication. The session continues until one of the devices sends an end of session signal or a time-out occurs, at which point the telemetry interlock is re-activated.

Fig. 3 depicts a communications session between the external device 2 and the implantable device 1 over a long-range telemetry channel in an embodiment using a telemetry interlock and where authentication is performed with public key cryptography. After the telemetry lock is released by an ENABLE command from the external device 3, the external device 2 transmits a message M1 encrypted by a public

key encryption algorithm using a key PubKey1 having a corresponding private key thought to be possessed by the implantable device. The implantable device responds by decrypting the message with the private key corresponding to PubKey1 to obtain M1 and transmitting M1 back to the implantable device encrypted by a public key PubKey2 having a corresponding private key thought to be possessed by the external device 2. When the external device 2 decrypts the message with its private key and obtains M1, the external device 2 has authenticated the implantable device 1, as the latter has evidenced possession of the private key corresponding to public key PubKey1. The implantable device 1 at the same time sends a message M2 also encrypted by public key PubKey2. The external device 2 responds by decrypting the message with the private key corresponding to public key PubKey2 to obtain M2 and transmitting M2 encrypted with public key PubKey1 back to the implantable device 1, thus authenticating the external device 2 to the implantable device. The external device 2 also transmits a secret session key SK encrypted by encrypted with public key PubKey1. A data communications session may then ensue using secret key cryptography in which DATA is transmitted by either of the devices encrypted with the secret session key SK. The session continues until one of the devices sends an end of session signal or a time-out occurs, at which point the telemetry interlock is re-activated.

Fig. 4 depicts a communications session using a more specific embodiment of the authentication protocol illustrated in Fig. 3. It is assumed that the external device 2 and the implantable device know each other's public authentication key. When an instigator (in this embodiment, the instigator is the external device 2) wants to establish an authenticated long-range telemetry session with an implantable device, it begins by encrypting its identity ID2 and a random number R_A with the implantable device's public key PubKey1. No listener except the intended recipient will be able to decrypt this information (even if the listener knows the recipient's public key) because no one except the intended recipient knows the recipient's private key. The recipient device decrypts this message with its private key. It then looks up the public key of the instigator PubKey2 and uses this to encrypt its identity ID1, the random number

R_A, and a second random number R_B. The recipient then transmits this encrypted information back to the instigator. Again, no one but the instigator is able to decrypt this information because no one but the instigator knows the instigator's private key. The instigator upon receiving back and verifying the random number it sent R_A, now knows that the implantable device it is communicating with is in fact the intended device, because only the intended device could have decrypted and returned R_A. The instigator then encrypts R_B with the recipient's public key PubKey1 and sends this back to the recipient. Upon receiving, decrypting, and verifying R_B, the recipient now knows that the instigator is in fact the holder of the correct private key, because only the holder of that private key could have decrypted and returned R_B. Authentication has now occurred. Both sides of the communication session now know that its communication partner holds the proper private key. Note that in this embodiment, recording the authentication exchanges and retransmitting parts of the exchanges in an attempt to impersonate an authorized device would not work because random numbers were used by both participants in the authentication, and these will be different each time.

Again, because a public key cryptographic algorithm is computationally expensive, it is only used in the embodiment of Fig. 4 for authentication at the start of each session, and the messages encrypted are of minimal size (typically a few hundred bits). The instigator transmits a secret session key SK encrypted with public key PubKey1 so that data communications session may be performed using secret key cryptography. In this embodiment, the secret session key SK is transmitted to the recipient device during authentication in the same frame that sends back R_B. In this way the number of frames using public key encryption is reduced by one (and public key encryption is very computationally expensive). In a particular embodiment, the secret session key SK is 64 bits. Although a 64-bit key is easier to decipher than the 128 bit public key, it is sufficient to provide security for the relative short duration of a typical telemetry session. The data communications session continues until one of the devices sends an end of session signal or a time-out occurs, at which point the telemetry interlock is re-activated. In another particular embodiment, the session key

expires at the end of each telemetry session, and a new key is chosen at random for the next session.

Even using secret key cryptography for data communications, it still may not be feasible for an implantable medical device to encrypt or decrypt every message that it sends or receives. It is not easy for the present generation of cardiac rhythm management devices to encrypt real-time electrograms without adding significant latency to the transmission. In one embodiment, therefore, the implantable medical device only encrypts selective data and sends other data in the clear. For example, only the most sensitive patient data (such as patient name, social security number and diagnosis) may be encrypted. An encryption flag in the header of each data packet could indicate if the contents are encrypted or not.

With either public key or secret key authentication, it is evidence of possession of a particular key which authenticates a device. In general, all authentication protocols are only as secure as the private keys in the case of public key cryptography and the secret keys in the case of secret key cryptography. For this reason the private or secret keys should be long (e.g., 128 bit in one embodiment). For added security, the private or secret key may be either hardwired into a device at the factory or generated internally by the device, and then prevented from being read out by telemetry. For example, a private key may be programmed into a device during manufacture, with its corresponding public key then included with the product documentation or obtainable through short-range inductive telemetry. A physician can then program the device's public key into a home monitor, a portable repeater, or a programmer. All external devices have unique public and private authentication keys as well, with the public key included with the product documentation. A physician can thus program a number of external device's public keys into an implantable device. In another embodiment, both implantable and external devices are capable of randomly generating new public/private key pairs by the RSA algorithm or through some other standard key pair generating algorithm. In this embodiment, new keys can be generated when the physician commands it via secure short-range inductive telemetry.

In a preferred embodiment, the authentication schemes described above only apply to the long-range telemetry link so that communication is always available in an emergency via short-range telemetry. For example, in case of a device reset, or some other fault that may cause the authentication keys to be corrupted, a long-range authenticated telemetry session will not be possible. In this case, short-range telemetry should still be available to reset the authentication keys. Another example of why short-range telemetry should be available without authentication is the traveling patient who needs device interrogation when away from his home physician.

Although the invention has been described in conjunction with the foregoing specific embodiment, many alternatives, variations, and modifications will be apparent to those of ordinary skill in the art. Such alternatives, variations, and modifications are intended to fall within the scope of the following appended claims.

What is claimed is:

1. A system for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

means for implementing a telemetry interlock which limits any communications between the ED and the IMD over the telemetry channel;

means for releasing the telemetry interlock by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD;

means for authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD;

means for authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

means for allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD and ED have been authenticated to one other.

2. A system for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

means for implementing a telemetry interlock which is released by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD; and,

means for limiting data communications between the IMD and ED over the telemetry channel until the telemetry interlock has been released.

3. The system of claim 2 wherein the short-range communications channel is an inductive communications link between the IMD and another device.

4. The system of claim 2 wherein the short-range communications channel is a switch within the IMD which is actuated by a magnet held in close proximity to the IMD to thereby release the telemetry interlock.

5. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

implementing a telemetry interlock which limits any communications between the ED and the IMD over the telemetry channel;

releasing the telemetry interlock by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD;

authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD;

authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD and ED have been authenticated to one other.

6. The method of claim 5 wherein the ED and the IMD are authenticated to one another using public key cryptography by:

authenticating the IMD to the ED when the ED encrypts a first message with a public key having a corresponding private key expected to be possessed by the IMD, transmits the encrypted first message over the telemetry channel to the IMD, and receives in response a message from the IMD derived from the first message which thereby evidences possession of the corresponding private key by the IMD; and,

authenticating the ED to the IMD when the IMD encrypts a second message with a public key having a corresponding private key expected to be possessed by the ED, transmits the encrypted second message over the telemetry channel to the ED, and

receives in response a message from the ED derived from the second message which thereby evidences possession of the corresponding private key by the ED.

7. The method of claim 6 wherein the message derived from the first message includes the first message and wherein the message derived from the second message includes the second message.

8. The method of claim 6 wherein the first and second messages include random numbers generated by the ED and IMD, respectively.

9. The method of claim 6 wherein the first and second messages include identity codes for the ED and IMD, respectively.

10. The method of claim 6 wherein the messages derived from the first and second messages and which are transmitted by the IMD and ED, respectively, are encrypted using the public keys of the ED and IMD, respectively.

11. The method of claim 6 wherein the message derived from the first message which is transmitted by the IMD includes the second message.

12. The method of claim 5 further comprising encrypting communications between the ED and IMD during the data communications session.

13. The method of claim 6 further comprising encrypting communications between the ED and IMD during the data communications session with secret key cryptography, wherein the secret key data communications session is established by one of either the ED or the IMD transmitting to the other of either the ED or the IMD a secret session key encrypted by the latter's public key.

14. The method of claim 5 wherein one of either the ED or the IMD is designated as a session instigator and the other of the ED or IMD is designated as a session recipient, the ED and the IMD are authenticated to one another using public key cryptography, and authentication is accomplished by:

the instigator encrypting a first message with a public key having a corresponding private key expected to be possessed by the recipient, wherein the first message includes an identity code for the instigator and a random number R_A,

the instigator transmitting the encrypted first message over the telemetry channel to the recipient;

the recipient decrypting the first message with its private key, looking up a public key having a corresponding private key expected to be possessed by the instigator using the identity code contained in the first message, and encrypting a second message with the public key of the instigator, wherein the second message includes an identity code for the recipient, the random number R_A, and a second random number R_B;

the recipient transmitting the encrypted second message over the telemetry channel to the instigator;

the instigator decrypting the second message with its private key corresponding to the public key used to encrypt the second message and verifying that the second message contains R_A to thereby authenticate the recipient;

the instigator encrypting a third message derived from the second message with the public key of the recipient, wherein the third message includes the random number R_B;

the instigator transmitting the encrypted third message over the telemetry channel to the recipient; and,

the recipient decrypting the third message with its private key corresponding to the public key used to encrypt the third message and verifying that the third message contains R_B to thereby authenticate the instigator.

15. The method of claim 14 further comprising encrypting communications between the instigator and the recipient during the data communications session with secret key cryptography, wherein the secret key data communications session is established by the instigator transmitting to the recipient a secret session key encrypted by the recipient's public key.

16. The method of claim 15 wherein the secret session key is contained in the third message transmitted by the instigator.

17. The method of claim 5 wherein the ED and the IMD are authenticated to one another using secret key cryptography by:

authenticating the IMD to the ED when the ED transmits a first message to the IMD over the telemetry channel and receives in response a message derived from the first message which is encrypted by a secret key expected to be possessed by the IMD;

authenticating the ED to the IMD when the IMD transmits a second message to the ED over the telemetry channel and receives in response a message derived from the second message which is encrypted by a secret key expected to be possessed by the ED.

18. The method of claim 5 wherein, after a data communications session ends, the telemetry interlock is re-activated to limit communications over the telemetry channel until the telemetry interlock is again released.

19. The method of claim 5 wherein no communications between the ED and IMD are allowed to occur until the telemetry interlock is released.

20. The method of claim 5 wherein a data communications session over the telemetry channel can be established which allows transmission of data from the IMD to the ED if the telemetry interlock is not released, but programming of the IMD by the ED cannot be performed unless the telemetry interlock is released.

21. The method of claim 5 wherein the telemetry channel is a far-field radio-frequency communications link.

22. The method of claim 5 wherein the telemetry channel includes an internet link.

23. The method of claim 5 wherein the short-range communications channel is an inductive communications link between the IMD and another device.

24. The method of claim 5 wherein the short-range communications channel is a switch within the IMD which is actuated by a magnet held in close proximity to the IMD to thereby release the telemetry interlock.

25. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

implementing a telemetry interlock which is released by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD; and,

limiting data communications between the IMD and ED over the telemetry channel until the telemetry interlock has been released.

26. The method of claim 25 wherein, after a data communications session over the telemetry channel ends, the telemetry interlock is re-activated to limit communications over the telemetry channel until the telemetry interlock is again released.

27. The method of claim 25 wherein no communications between the ED and IMD are allowed to occur over the telemetry channel until the telemetry interlock is released.

28. The method of claim 25 wherein a data communications session over the telemetry channel can be established which allows transmission of data from the IMD to the ED if the telemetry interlock is not released, but programming of the IMD by the ED cannot be performed unless the telemetry interlock is released.

29. The method of claim 25 wherein the short-range communications channel is an inductive communications link between the IMD and another device.

30. The method of claim 25 wherein the short-range communications channel is a switch within the IMD which is actuated by a magnet held in close proximity to the IMD to thereby release the telemetry interlock.

31. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD has been authenticated to the ED.

32. The method of claim 31 further comprising:

authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD and ED have been authenticated to one other.

33 The method of claim 32 wherein the ED and the IMD are authenticated to one another using public key cryptography by:

authenticating the IMD to the ED when the ED encrypts a first message with a public key having a corresponding private key expected to be possessed by the IMD, transmits the encrypted first message over the telemetry channel to the IMD, and receives in response a message from the IMD derived from the first message which thereby evidences possession of the corresponding private key by the IMD; and,

authenticating the ED to the IMD when the IMD encrypts a second message with a public key having a corresponding private key expected to be possessed by the ED, transmits the encrypted second message over the telemetry channel to the ED, and receives in response a message from the ED derived from the second message which thereby evidences possession of the corresponding private key by the ED.

34. The method of claim 32 wherein the ED and the IMD are authenticated to one another using secret key cryptography by:

authenticating the IMD to the ED when the ED transmits a first message to the IMD over the telemetry channel and receives in response a message derived from the first message which is encrypted by a secret key expected to be possessed by the IMD;

authenticating the ED to the IMD when the IMD transmits a second message to the ED over the telemetry channel and receives in response a message derived from the second message which is encrypted by a secret key expected to be possessed by the ED.

35. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the ED has been authenticated to the IMD.

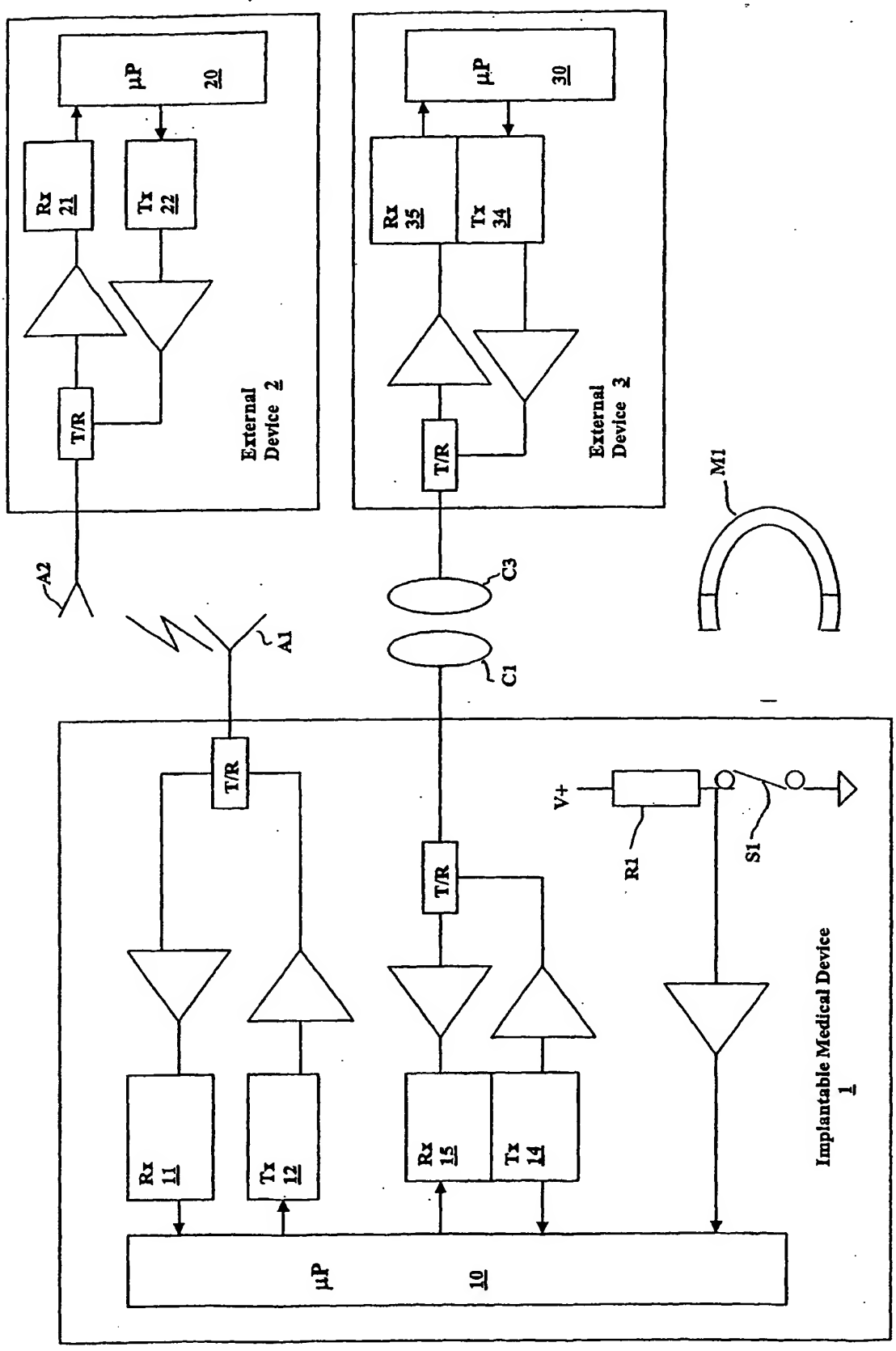

μP 20
Rx 21
Tx 22
T/R
External Device 2
μP 30
Rx 35
Tx 34
T/R
External Device 3
M1
A2
A1
C3
C1
T/R
T/R
V+
R1
S1
Rx 11
Tx 12
Rx 15
Tx 14
μP 10
Implantable Medical Device 1

Fig. 1

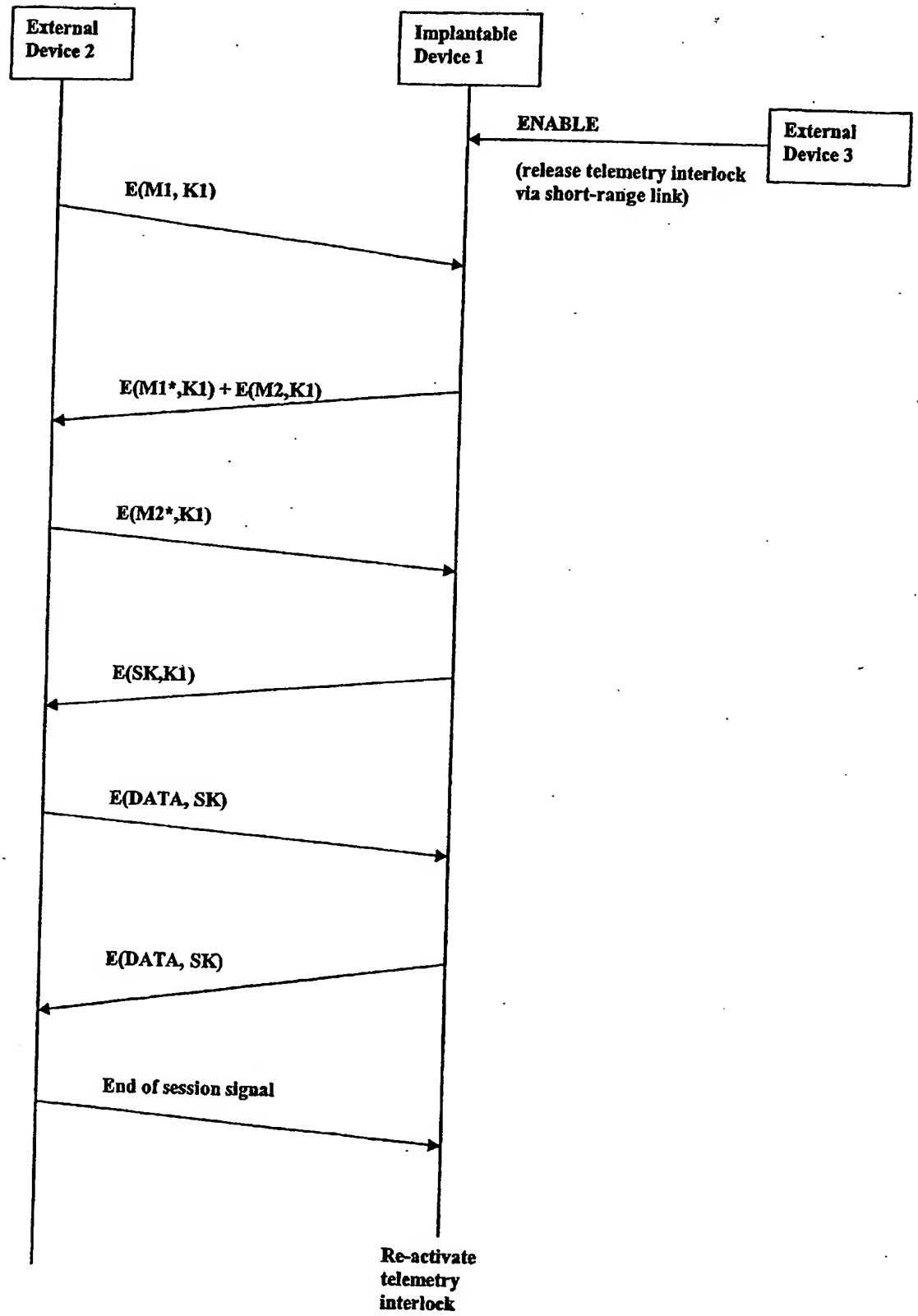

External Device 2
Implantable Device 1
ENABLE
External Device 3
(release telemetry interlock via short-range link)
E(M1, K1)
E(M1*,K1) + E(M2,K1)
E(M2*,K1)
E(SK,K1)
E(DATA, SK)
E(DATA, SK)
End of session signal
Re-activate telemetry interlock

Fig. 2

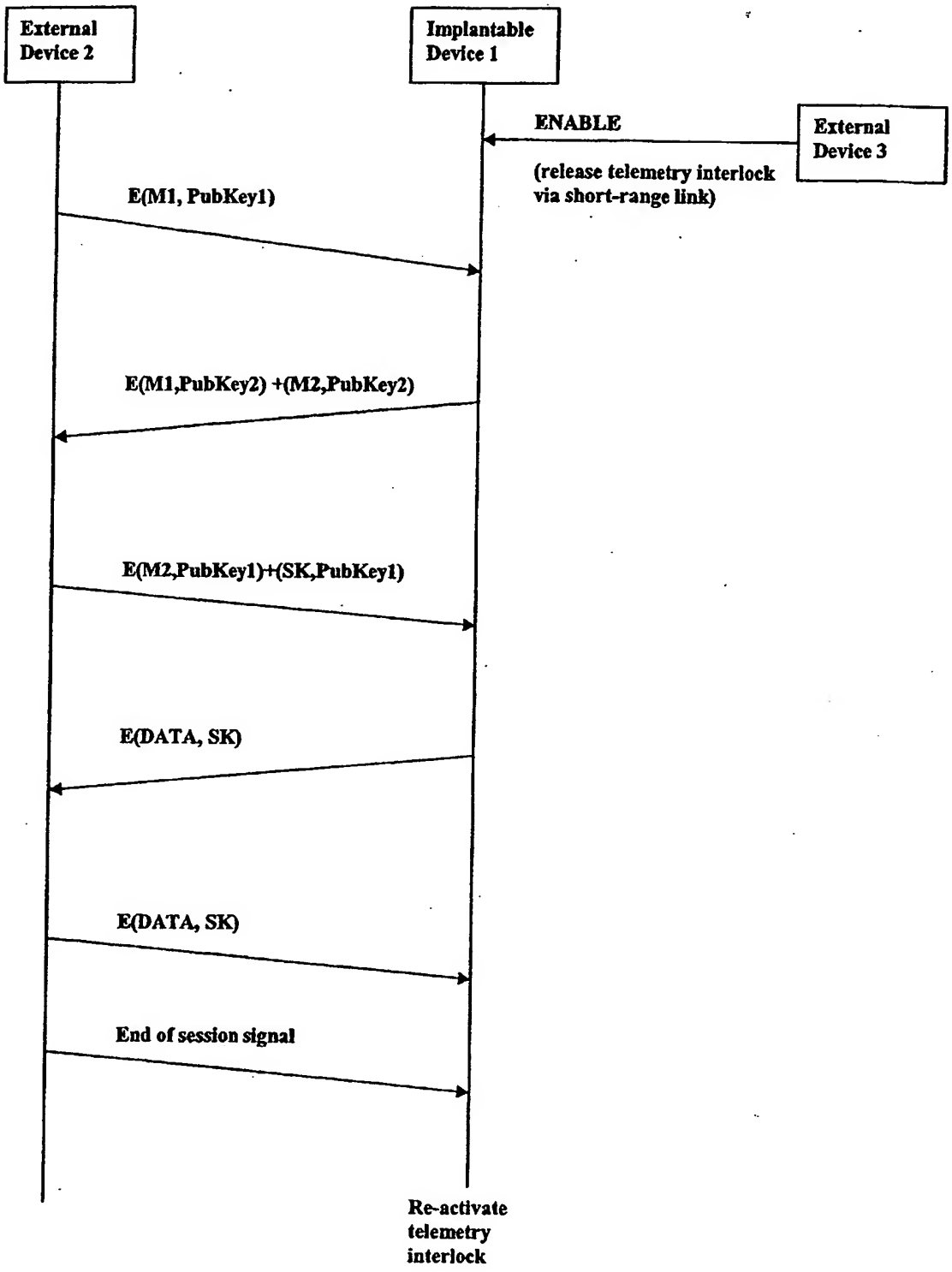

External Device 2
Implantable Device 1
ENABLE
External Device 3
(release telemetry interlock via short-range link)
E(M1, PubKey1)
E(M1,PubKey2) +(M2,PubKey2)
E(M2,PubKey1)+(SK,PubKey1)
E(DATA, SK)
E(DATA, SK)
End of session signal
Re-activate telemetry interlock

Fig. 3

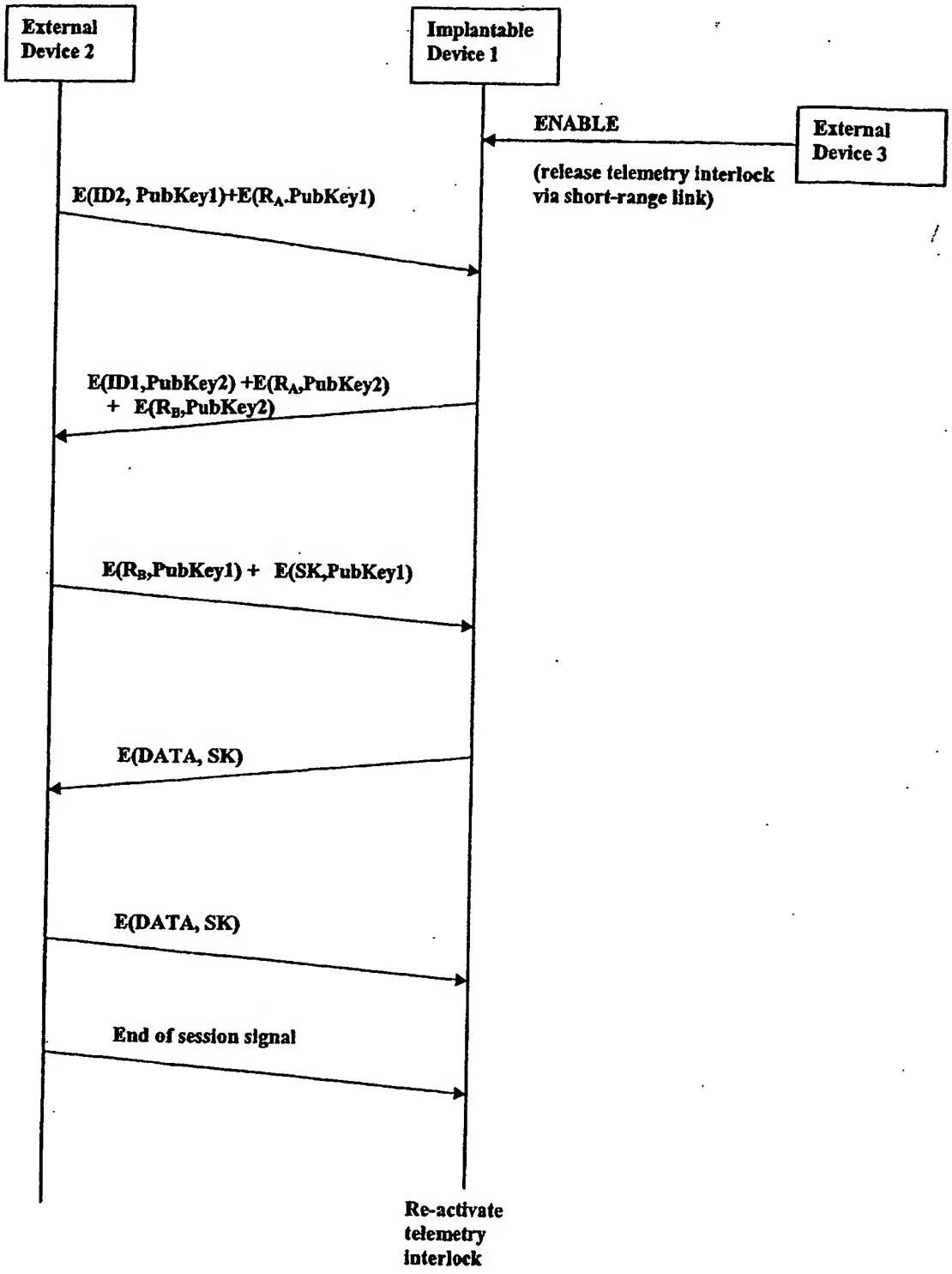

External Device 2
Implantable Device 1
ENABLE
External Device 3
(release telemetry interlock via short-range link)
E(ID2, PubKey1)+E(R_A.PubKey1)
E(ID1,PubKey2) +E(R_A,PubKey2) + E(R_B,PubKey2)
E(R_B,PubKey1) + E(SK,PubKey1)
E(DATA, SK)
E(DATA, SK)
End of session signal
Re-activate telemetry interlock

Fig. 4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/019902

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 A61N1/372 A61N1/08 A61B5/00 G06F19/00 H04L9/30
H04L9/32 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 A61N H04L A61B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
X	US 2003/114898 A1 (VON ARX JEFFREY A ET AL) 19 June 2003 (2003-06-19)	1-3,5, 12-16, 18,19, 21,23, 25-27, 29,31, 32,35
Y		6-11,17, 22,33,34
A	p. 1, '0006! - p. 9, '0085!; figures 1,2,5-8	4,20,24, 28,30

-/--

[X] Further documents are listed in the continuation of box C

[X] Patent family members are listed in annex

* Special categories of cited documents

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 2004	06/12/2004

Name and mailing address of the ISA
European Patent Office, P B 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Tx 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer
Fischer, O

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/019902

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
Y A	US 2001/027331 A1 (THOMPSON DAVID L) 4 October 2001 (2001-10-04) p. 4, '0027! - p. 7, '0048!; figures 1-5	6-11,17, 22,33,34 1-5, 12-16, 18-21, 23-32,35
A	US 6 434 429 B1 (NAGELSCHMIDT AXEL ET AL) 13 August 2002 (2002-08-13) column 2, line 59 - column 6, line 26 column 10, line 46 - column 16, line 31; figures 1,2,5,7	1-5, 18-32,35
A	US 2002/147388 A1 (ARX JEFFREY A VON ET AL) 10 October 2002 (2002-10-10) p. 1, '0007! - p. 3, '0023!; figures 1-4	1-5, 18-32,35
A	US 6 385 318 B1 (OISHI KAZUOMI) 7 May 2002 (2002-05-07) abstract; figures 1-4	1,5-17, 31-35

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/019902

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003114898 A1	19-06-2003	NONE	
US 2001027331 A1	04-10-2001	NONE	
US 6434429 B1	13-08-2002	DE 19930256 A1	28-12-2000
		EP 1062985 A2	27-12-2000
US 2002147388 A1	10-10-2002	EP 1404409 A2	07-04-2004
		WO 03095023 A2	20-11-2003
US 6385318 B1	07-05-2002	JP 9284272 A	31-10-1997
		AU 1898097 A	23-10-1997
		CN 1177245 A	25-03-1998
		DE 69731025 D1	11-11-2004
		EP 0802654 A2	22-10-1997